Part A Number Theory 2020

Ben Green

Contents

Preface

These are notes for an 8-lecture first course in number theory, taught in Oxford as a Part A short option course. The notes were comprehensively rewritten in 2017, but it was useful to have access to the earlier notes developed by Alan Lauder, Tim Browning, Andrew Cadwell, Roger Heath-Brown, Henri Johnston and Jennifer Balakrishnan. Please address any comments and corrections to

ben.green@maths.ox.ac.uk

Synopsis. The ring of integers; congruences; ring of integers modulo n ; the Chinese Remainder Theorem. Wilson's Theorem; Fermat's Little Theorem for prime modulus; Euler's phi-function. Euler's generalisation of Fermat's Little Theorem to arbitrary modulus; primitive roots. Quadratic residues modulo primes. Quadratic reciprocity. Factorisation of large integers; basic version of the RSA encryption method.

Non-examinable topics are denoted with an asterisk.

Notation. If m, n are two positive integers, then I like to write (m, n) for the highest common factor of m and n. This is pretty standard notation, and is almost ubiquitous in research papers. Some authors write $\mathrm{hcf}(m, n)$ or $\gcd(m, n)$; you may find this in past exam papers.

Although we will not use it in this course, I write $[m, n]$ for the lowest common multiple of m and n. Some authors use $\mathrm{lcm}(m, n)$ or, worse still, $l.c.m.(m, n)$.

CHAPTER 1

Some basics

We begin by going over a few basic facts about the ring of integers $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2 \dots\}$. Most of these have already been covered in the Prelims course Constructive Mathematics or the Part A course Rings and Modules.

1.1. Euclid's algorithm

If a, b are integers then the highest common factor, denoted by (a, b) in this course, is the largest *positive* integer d satisfying $d|a$ and $d|b$.

PROPOSITION 1.1 (Euclid's algorithm). *Suppose that a, b are integers. Then there are integers m, n such that $am + bn = (a, b)$.*

Proof. Replacing a by $-a$ and b by $-b$ and switching the role of a, b if necessary, we may assume that $a \geqslant b \geqslant 0$. Now perform Euclid's algorithm:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_k &= q_{k+2} r_{k+1} + 0, \end{aligned}$$

where the quotients q_i are nonnegative integers and the remainders r_i are nonnegative and satisfy $r_{i+1} < r_i$. This last property guarantees that the algorithm does terminate.

We claim that $(a, b) = r_{k+1}$. Inducting up from the bottom, we have that r_{k+1} divides, in sequence, $r_k, r_{k-1}, \dots, r_1, b, a$. Thus $r_{k+1}|(a, b)$. If $d|a, b$ then, working downwards from the top, d divides $a, b, r_1, \dots, r_{k+1}$. In particular $(a, b)|r_{k+1}$. It follows that $(a, b) = r_{k+1}$.

Now we have, working up from the bottom,

$$\begin{aligned}(a,b) &= r_{k+1}\\ &= r_{k-1} - q_{k+1}r_k\\ &= r_{k-1} - q_{k+1}(r_{k-2} - q_k r_{k-1})\\ &\vdots\\ &= ma + nb\end{aligned}$$

for some integers m, n. □

The proof provides an algorithm for finding m, n. This has been covered in the Prelims course Constructive Mathematics, and there are some examples on the exercise sheets to refresh your memory.

1.2. Units, irreducibles and primes

The *units* in $\mathbb{Z}$ are 1 and -1. These are the only integers m which have a multiplicative inverse, that is to say for which there is another integer n such that $mn = 1$.

We say that an integer p is *irreducible* if it is not a unit, and if it has no factors other than $\pm 1, \pm p$.

We say that an integer p is *prime* if it is not a unit and if it has the following property: if $p|ab$ then either $p|a$ or $p|b$.

PROPOSITION 1.2. *An integer p is irreducible if and only if it is prime.*

Proof. Suppose first that p is prime. We claim that p is irreducible. Suppose not; then $p = ab$ with neither a nor b a unit. Since p is prime, either $p|a$ or $p|b$. Suppose without loss of generality that $p|a$. Thus $a = pc$ for some $c \in \mathbb{Z}$. But then $p = ab = pbc$, so $p(1 - bc) = 0$. It follows that $1 - bc = 0$ (here we used the fact that $\mathbb{Z}$ is an *integral domain*) and hence $bc = 1$, contrary to the supposition that b was not a unit.

Now suppose that p is irreducible, and that $p|ab$. Suppose that $p \nmid a$. Then the highest common factor of a and p is 1. By Euclid's algorithm, there are m, n such that $ma + np = 1$, and hence $mab + npb = b$. Observe that p divides the left-hand side, and hence $p|b$. □

The reason for the strange-seeming nomenclature – using two different words for the same thing – is that there are other rings (for example $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$) where the notions of prime and irreducible do *not* coincide. There is

much more on this in the Part A course Rings and Modules. In this course we will only be working over $\mathbb{Z}$, so we use the word "prime" instead of irreducible.

PROPOSITION 1.3. *Every integer other than zero and the units may be factored into primes in an essentially unique way.*

Proof. By "essentially unique" we mean that the factorisations $15 = (-3)(-5) = 5 \cdot 3 = 3 \cdot 5$ are all regarded as the same: more formally, factorisations are unique up to reordering the primes and modifying them by the units ± 1.

Let n be an integer. First we show that n can be written as a product of primes. It may be that n is already irreducible. If not, we may split it as a product $n = ab$ of two integers a, b with $1 < |a|, |b| < |n|$. This allows us to proceed by induction on $|n|$.

Now we show that factorisations are unique. Suppose that

$$n = p_1 \dots p_k = q_1 \dots q_m.$$

We have $p_1 | q_1 \dots q_m$, and so p_1 divides one of the q_i. Relabelling, we may suppose that $p_1 | q_1$. Since p_1, q_1 are primes, we must have $p_1 = uq_1$, for some unit u, and hence

$$p_2' \dots p_k = q_2 \dots q_m$$

where $p_2' = up_2$. Continuing inductively gives the result. □

It is important to remark that the uniqueness of decomposition into primes, which you have probably known since you were at primary school, is not obvious! In fact, it fails in most rings (such as $\mathbb{Z}[\sqrt{-5}]$).

1.3. GCD and LCM. Coprimality.

Let us recall the definitions. If a, b are integers then the greatest common divisor (GCD) of a and b, written (a, b), is the greatest *positive* integer d such that $d|a$ and $d|b$. The lowest common multiple (LCM), written $[a, b]$, is the least positive integer d such that $a|d$ and $b|d$. We say that a and b are *coprime* if $(a, b) = 1$, or equivalently if there does not exist a prime p dividing both a and b. More generally, we say that integers $a_1, \dots, a_k$ are *pairwise coprime* if $(a_i, a_j) = 1$ for all $i \neq j$, or equivalently if no prime p divides more than one of the a_i.

Remark. One could say that $a_1, \dots, a_k$ are coprime if there is no prime p dividing all of $a_1, \dots, a_k$. This is a weaker condition than pairwise coprimality, and it will not come up much in this course. (For example, $2, 5$ and 10 are coprime, but not pairwise coprime; and even worse example is $6, 10$ and 15, which are coprime but for which *none* of the pairs is coprime.)

Here are some facts about GCDs, LCMs and coprimality that come up repeatedly in the course. The proofs all follow straightforwardly from unique factorisation into primes, and the details are left to the student.

LEMMA 1.1. *We have the following facts.*

(i) *Suppose that a, b are positive and that $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ and $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$, where the p_i are distinct primes. Then $(a, b) = p_1^{\min(\alpha_1,\beta_1)} \cdots p_k^{\min(\alpha_k,\beta_k)}$, and $[a, b] = p_1^{\max(\alpha_1,\beta_1)} \cdots p_k^{\max(\alpha_k,\beta_k)}$. In particular $ab = [a, b](a, b)$.*

(ii) *Suppose that a, b are coprime and that $b|ax$. Then $b|x$.*

(iii) *Suppose that $q_1, \ldots, q_k$ are pairwise coprime. Then $q_1 \cdots q_k$ divides x if and only if q_i divides x for $i = 1, \ldots, k$.*

(iv) *Suppose that a and b are both coprime to q. Then so is ab.*

1.4. Linear diophantine equations

In this section we record the general result about solving the equation $am+bn = c$ in integers. (An equation to be solved in integers is called a Diophantine equation, hence the title of the section.) First, we need a lemma which follows from the results of the last section.

PROPOSITION 1.4. *Suppose that a, b, c are integers with $a, b \neq 0$. Then there is a solution to the equation $am + bn = c$ in integers m, n if and only if $(a, b)|c$. Two integers m', n' give another solution if and only if $m' = m+k\frac{b}{(a,b)}$ and $n' = n-k\frac{a}{(a,b)}$ for some integer k.*

Proof. It is obvious that *if* the equation is soluble then (a, b) divides c. Conversely, by Euclid's algorithm we see that if $(a, b)|c$ then the equation does have a solution: take a solution to $au + bv = (a, b)$ and set $m = \frac{c}{(a,b)}u$ and $n = \frac{c}{(a,b)}v$.

For the last part, observe that if we write $x = m' - m$ and $y = n - n'$ then $am' + bn' = c$ if and only if $ax = by$. Dividing through by (a, b) gives $a'x = b'y$, where $a' = \frac{a}{(a,b)}$ and $b' = \frac{b}{(a,b)}$. Note that a' and b' are now coprime. If follows from Lemma 1.1 (ii) that $b'|x$ and that $a'|y$. Writing $x = b'k_1$ and $y = a'k_2$, it follows immediately that $k_1 = k_2$, and this tells us that m', n' have the form claimed. Conversely if m', n' do have this form then it is trivial to check that $am' + bn' = c$. □

1.5. The infinitude of primes

PROPOSITION 1.5. *The are infinitely many primes.*

Proof. Suppose that a complete list of primes is $\{p_1, \ldots, p_k\}$. Consider the number $N := p_1p_2 \cdots p_k + 1$. This must certainly have a prime factor. However, it is easy

to see that none of the primes $p_1, \ldots, p_k$ divides N, which leaves a remainder of 1 upon division by any of these primes. $\square$

CHAPTER 2

Modular arithmetic and $\mathbb{Z}/q\mathbb{Z}$

2.1. Modular arithmetic

When divided by 4, the number 2019 leaves a remainder of 3. We usually write this as $2019 \equiv 3 (\mathrm{mod}\, 4)$ and we say that 2019 is *congruent to* 3 *mod* 4.

Every square number is congruent to 0 or 1 mod 4 (there are two cases: either $n = 2k$ in which case $n^2 = 4k^2$, or $n = 2k + 1$, in which case $n^2 = 4(k^2 + k) + 1$).

Therefore every sum of two squares is congruent to 0, 1 or 2 mod 4, and it follows that 2019 is not the sum of two squares.

To give another example, we have $365 \equiv 1 (\mathrm{mod}\, 7)$, which explains why April 26th is a Thursday this year, but will be a Friday next.

These are "modular arithmetic" arguments. The remainder does not have to be the *least* remainder. Thus it is also OK to write $2019 \equiv 11 (\mathrm{mod}\, 4)$, and $2019 \equiv -1 (\mathrm{mod}\, 4)$.

Definition 2.1. Let $q \geqslant 1$ be an integer. Then we write $a \equiv b (\mathrm{mod}\, q)$ if and only if q divides $a - b$.

We implicitly used some basic facts about modular arithmetic which we have not proved carefully, namely the first part of the following lemma.

Lemma 2.1. *Suppose that* $x \equiv a (\mathrm{mod}\, q)$ *and that* $y \equiv b (\mathrm{mod}\, q)$. *Then* $x + y \equiv a + b (\mathrm{mod}\, q)$ *and* $xy \equiv ab (\mathrm{mod}\, q)$.

Proof. The first part is rather easy and is left as an exercise. For the second part, suppose that $x \equiv a (\mathrm{mod}\, q)$ and that $y \equiv b (\mathrm{mod}\, q)$. Then $x = a + kq$ and $y = b + k'q$ for integers k, k'. It follows that

$$xy = (a + kq)(b + k'q) = ab + q(kb + k'a + qkk'),$$

and so indeed $xy \equiv ab (\mathrm{mod}\, q)$. □

Another very basic fact about modular arithmetic is *cancellation*.

Corollary 2.1. *Suppose that* $ac \equiv bc (\mathrm{mod}\, q)$, *and that* q *is coprime to* c. *Then* $a \equiv b (\mathrm{mod}\, q)$.

Proof. The assumption implies that $q|c(a-b)$. Applying Lemma 1.1 (ii) tells us that $q|a-b$, and so $a \equiv b (\mathrm{mod}\, q)$. □

Remark. For the avoidance of doubt, it should be very clearly pointed out that the hypothesis that q is coprime to c is essential. For example, $2\times 5 \equiv 4\times 5 (\mathrm{mod}\, 10)$, but of course $2 \not\equiv 4 (\mathrm{mod}\, 10)$.

2.2. The ring $\mathbb{Z}/q\mathbb{Z}$

The fact that "$(\mathrm{mod}\, q)$" works well with regard to both addition and multiplication is really asserting some properties of a natural *ring homomorphism* from the integers $\mathbb{Z}$ to a ring called $\mathbb{Z}/q\mathbb{Z}$.

The relation $\sim$, defined by $x \sim y$ if and only if $x \equiv y (\mathrm{mod}\, q)$, is easily seen to be an equivalence relation. The equivalence classes are precisely the sets $x+q\mathbb{Z} = \{x+kq : k \in \mathbb{Z}\}$, that is to say the cosets of the subgroup $q\mathbb{Z} = \{\dots, -q, 0, q, 2q, \dots\} \subset \mathbb{Z}$. For this introductory discussion (when the value of q is clear from context, and there is no danger of confusion with other notations) we write $\overline{x} = x + q\mathbb{Z}$. Some authors would write $x (\mathrm{mod}\, q)$ for the same thing.

A complete set of distinct equivalence classes is $\{\overline{0}, \overline{1}, \cdots, \overline{q-1}\}$; after $\overline{q-1}$ we start to repeat, thus $\overline{q} = \overline{0}$, $\overline{q+1} = \overline{1}$, and so on, and also $\overline{-1} = \overline{q-1}$, $\overline{-2} = \overline{q-2}$, and so on. We write $\mathbb{Z}/q\mathbb{Z}$ for this set of equivalence classes.

Example. We have $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$ or, more formally, $\{0+3\mathbb{Z}, 1+3\mathbb{Z}, 2+3\mathbb{Z}\}$. Since $7 \equiv -2 (\mathrm{mod}\, 3)$, we have $\overline{7} = \overline{-2}$ or, more formally, $7 + 3\mathbb{Z} = -2 + 3\mathbb{Z}$.

Lemma 2.1 implies that $\mathbb{Z}/q\mathbb{Z}$ has the structure of a ring (with 1), with a well-defined addition given by

$$(x + q\mathbb{Z}) + (y + q\mathbb{Z}) = (x + y) + q\mathbb{Z}$$

and a well-defined multiplication given by

$$(x + q\mathbb{Z})(y + q\mathbb{Z}) = xy + q\mathbb{Z}.$$

(the role of Lemma 2.1 here is that, for example, $x + q\mathbb{Z}$ does not uniquely specify x; we have $x + q\mathbb{Z} = a + q\mathbb{Z}$ whenever $x \equiv a (\mathrm{mod}\, q)$.) The zero in this ring is $0 + q\mathbb{Z} = q\mathbb{Z}$, and the multiplicative identity is $1 + q\mathbb{Z}$.

Moreover, the map $\pi : \mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ which sends $x \in \mathbb{Z}$ to $x + q\mathbb{Z}$ is a ring homomorphism.

Example. We have $(4 + 6\mathbb{Z}) \times (5 + 6\mathbb{Z}) = 2 + 6\mathbb{Z}$.

Remark. Let us say a few words about the correct generality for this construction. It is an example of a more general construction of a quotient ring R/I, where

R is a commutative ring with identity 1_R and I is an ideal, that is to say a subset of R closed under addition and taking inverses, and with the property that

$$ri \in I \text{ whenever } r \in R \text{ and } i \in I. \tag{2.1}$$

In our example, $R = \mathbb{Z}$ and I is the ideal $q\mathbb{Z} = \{\dots, -2q, -q, 0, q, 2q, \dots\}$.

Note that I is a normal subgroup of R under $+$, and so the set of cosets

$$r + I \in R/I$$

is an (abelian) group under the addition

$$(r + I) + (s + I) := (r + s) + I$$

for $r, s \in R$. One checks also that the multiplication

$$(r + I) \times (s + I) := (r \times s) + I$$

is well-defined on the cosets in R/I by property (2.1). Thus R/I has the structure of a commutative ring with identity $1_R + I$.

Note that there is a natural quotient homomorphism $\pi : R \to R/I$ given by $\pi(r) = r + I$.

2.3. The multiplicative group. Inverses.

Let c be an integer. Whether or not c is coprime to q depends only on $c (\mathrm{mod}\, q)$. Therefore it makes sense to define

$$(\mathbb{Z}/q\mathbb{Z})^\times := \{x + q\mathbb{Z} \in \mathbb{Z}/q\mathbb{Z} : (x, q) = 1\} = \{\overline{x} : (x, q) = 1\}.$$

This is called the *multiplicative group of residues mod q*. For example,

$$(\mathbb{Z}/6\mathbb{Z})^\times = \{\overline{1}, \overline{5}\}, \quad (\mathbb{Z}/12\mathbb{Z})^\times = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}, \quad (\mathbb{Z}/11\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \cdots, \overline{10}\}.$$

LEMMA 2.2. *The multiplicative group $(\mathbb{Z}/q\mathbb{Z})^\times$ is indeed a group under multiplication.*

Proof. There is an identity element, namely $1 + q\mathbb{Z}$.

We must check that $(\mathbb{Z}/q\mathbb{Z})^\times$ is closed under multiplication, and also that inverses exist. The former amounts to the statement that if a, b are coprime to q then so is ab, which is Lemma 1.1 (iv).

To show the existence of inverses, suppose that $c + q\mathbb{Z} \in (\mathbb{Z}/q\mathbb{Z})^\times$. Then c is coprime to q. By Euclid's algorithm, there are integers m, n such that $cm + qn = 1$, and so $cm \equiv 1 (\mathrm{mod}\, q)$. Then m is coprime to q, and moreover $(c + q\mathbb{Z})(m + q\mathbb{Z}) = 1 + q\mathbb{Z}$ and so $m + q\mathbb{Z}$ is inverse to c. □

Remark. If $x \in \mathbb{Z}/q\mathbb{Z}$, then the inverse of x is usually denoted by $\overline{x}$, although we will not need this notation in the course. Obviously it is in conflict with the notation we introduced in Section 2.2 for the elements of $\mathbb{Z}/q\mathbb{Z}$. For that reason, the notation of that section is not normally used beyond an introductory course on modular arithmetic. In our course, it is limited to this section and the last.

2.4. The Chinese Remainder Theorem.

Here is the Chinese remainder theorem as usually stated.

THEOREM 2.1 (Chinese Remainder Theorem). *Suppose that $q_1, q_2, \ldots, q_k$ are pairwise coprime positive integers (that is, $(q_i, q_j) = 1$ for all $i \neq j$). Suppose that $a_1, \ldots, a_k$ are integers. Then there is an integer x such that $x \equiv a_i (\mathrm{mod}\, q_i)$ for $i = 1, 2, \ldots, k$. Moreover, x is unique $(\mathrm{mod}\, q_1 \cdots q_k)$.*

For example, there is an integer satisfying $x \equiv 3 (\mathrm{mod}\, 7)$ and $x \equiv 2 (\mathrm{mod}\, 5)$, namely $x = 17$, and this is unique $(\mathrm{mod}\, 35)$ (that is, x' also satisfies this condition if and only if $x' \equiv x (\mathrm{mod}\, 35)$).

Remark. The result is, in general, false if the q_i are not coprime. or example, there is no integer x such that $x \equiv 1 (\mathrm{mod}\, 4)$ and $x \equiv 3 (\mathrm{mod}\, 8)$.

The following is a more grown-up statement of the Chinese remainder theorem, equivalent to Theorem 2.1.

THEOREM 2.2. *Suppose that $q_1, \ldots, q_k$ are pairwise coprime. Then the map*

$$\psi : \mathbb{Z}/q_1 \cdots q_k\mathbb{Z} \to \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_k\mathbb{Z}$$

given by

$$\psi(x + q_1 \cdots q_k\mathbb{Z}) = (x + q_1\mathbb{Z}, \ldots, x + q_k\mathbb{Z})$$

is a bijection.

Proof. First we should remark that the map ψ is well-defined. This is a consequence of the fact that $x \equiv y (\mathrm{mod}\, q_1 \cdots q_k)$ implies that $x \equiv y (\mathrm{mod}\, q_i)$ for each i.

The domain and range of ψ have the same cardinality $q_1 \cdots q_k$. Hence, to show that ψ is a bijection, it suffices to show that it is an injection. But if $\psi(x) = \psi(y)$ then $q_i | y - x$ for each i and hence, since the q_i are pairwise coprime, $q_1 \cdots q_k | x - y$, which means that $x \equiv y (\mathrm{mod}\, q_1 \cdots q_k)$. □

In fact the proof gives rather more: $\mathbb{Z}/q_1 \cdots q_k\mathbb{Z}$ and $\mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_k\mathbb{Z}$ are isomorphic as rings. This is because ψ is easily seen to be a ring isomorphism, and hence, since it is bijective, is an isomorphism.

Whilst the proof of the Chinese Remainder Theorem is quite straightforward, it is nonconstructive: we are left with no clue as to how to actually solve the system of congruences $x \equiv a_i (\mathrm{mod}\, q_i)$ described in Theorem 2.1. Here is a way to construct an x explicitly (which also gives a second proof of the Chinese Remainder Theorem). For each $i \in \{1, \ldots, k\}$, write

$$Q_i := \frac{q_1 q_2 \cdots q_k}{q_i} = q_1 \cdots q_{i-1} q_{i+1} \cdots q_k.$$

Since the q_i are pairwise coprime, Q_i is coprime to q_i. Let m_i be any integer inverse to Q_i in $(\mathbb{Z}/q_i\mathbb{Z})^\times$: thus $m_i Q_i \equiv 1 (\mathrm{mod}\, q_i)$. Note that such an m_i can be constructed via the Euclidean algorithm. Finally, set

$$x = a_1 m_1 Q_1 + \cdots + a_k m_k Q_k.$$

Observe that all of the Q_i except for Q_1 are divisible by q_1. Therefore

$$x \equiv a_i m_i Q_i \equiv a_i (\mathrm{mod}\, q_i).$$

Once again, we should remark that x is not unique. In fact it is easy to see that y is another solution if and only if $q_1 \ldots q_k | y - x$.

Let us conclude with an example.

Example. Find an integer x such that $x \equiv 5 (\mathrm{mod}\, 11)$ and $x \equiv 11 (\mathrm{mod}\, 31)$.

Solution. Here, $q_1 = 11$ and $q_2 = 31$; these are certainly coprime. With the notation above, we have $Q_1 = 31$ and $Q_2 = 11$. To find an inverse for $31 (\mathrm{mod}\, 11)$, first reduce mod 11; we need to find an inverse for $9 (\mathrm{mod}\, 11)$. The Euclidean algorithm gives $1 = 5 \cdot 9 - 4 \cdot 11$, and so such an inverse is 5. Set $m_1 = 5$. To find an inverse for $11 (\mathrm{mod}\, 31)$, we again use the Euclidean algorithm, finding that $1 = 5 \cdot 31 - 14 \cdot 11$, so that an inverse for $11 (\mathrm{mod}\, 31)$ is -14. Set $m_2 = -14$.

Finally, take

$$x = 5 \cdot 5 \cdot 31 + 11 \cdot (-14) \cdot 11 = -919.$$

Adding $3 \cdot 341 = 1023$, we obtain the smallest positive solution

$$x = 104.$$

2.5. Fermat's Little Theorem

THEOREM 2.3. *Let p be a prime, and suppose that a is not a multiple of p. Then $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.*

Proof. Here is the traditional proof. Consider the numbers $a, 2a, \ldots, (p-1)a$ modulo p. These are mutually incongruent $(\mathrm{mod}\, p)$, as $ia \equiv ja (\mathrm{mod}\, p)$ implies $p | a(i-j)$, which implies that $i \equiv j (\mathrm{mod}\, p)$. None of these numbers is divisible by p. It follows that they must be precisely $1, 2, \ldots, p-1$ in some order. Taking

products, we obtain

$$a^{p-1}(p-1)! = a(2a)(3a)\cdots((p-1)a) \equiv 1\cdot 2\cdots(p-1) = (p-1)!.$$

By the cancellation lemma (Corollary 2.1), the result follows.

However, the result also follows from the well-known fact in finite group theory that the order of any element x in a finite group G divides $|G|$, which itself follows immediately from Lagrange's theorem (that the order of a subgroup divides the order of the group). Fermat's Little Theorem corresponds to the case $G = (\mathbb{Z}/p\mathbb{Z})^\times$, a group of order $p-1$: if $x+p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^\times$, then $x^{p-1}+p\mathbb{Z} = (x+p\mathbb{Z})^{p-1} = 1+p\mathbb{Z}$. □

Remark If $x^{p-1} \equiv 1 \pmod p$ for some $x \in \mathbb{Z}$ it does not imply that p is prime: for example, $2^{340} \equiv 1 (\mathrm{mod}\, 341)$, but $341 = 11\cdot 31$. The number 341 is an example of a *pseudoprime* to base 2: an odd number n satisfying $2^{n-1} \equiv 1 (\mathrm{mod}\, n)$, but for which n is not prime. Whilst there are infinitely many pseudoprimes, it is known that they are far rarer than primes. Thus if one computes that $2^{n-1} \equiv 1 (\mathrm{mod}\, n)$ then one can be fairly sure that n is prime (and if one computes $2^{n-1} \neq 1 (\mathrm{mod}\, n)$, where n is odd, then one can be *certain* that n is composite).

One might think that this is a completely useless observation, since 2^{n-1} will generally be a huge number and very difficult to compute. However, it can be computed efficiently $(\mathrm{mod}\, n)$ by repeated squaring: find $2, 2^2, 2^{2^2}, 2^{2^3}, \ldots (\mathrm{mod}\, n)$ in turn (each is the square of the previous one, and may then be reduced mod n), then multiply appropriate elements of this sequence together according to the binary expansion of $n-1$ to find $2^{n-1} (\mathrm{mod}\, n)$.

2.6. Wilson's Theorem

THEOREM 2.4. *Let p be an odd prime. Then $(p-1)! \equiv -1 (\mathrm{mod}\, p)$.*

Proof. In the product $(p-1)! = 1\cdot 2\cdots(p-1)$, group the elements in pairs, c together with its inverse $\overline{c} = c^{-1} (\mathrm{mod}\, p)$. Each pair contributes $1 (\mathrm{mod}\, p)$ to the product. Only two elements do not belong to a pair: 1 and -1 (because for these values of c, $\overline{c} = c$). Evidently the product of these two elements is -1. □

Remark. Wilson's theorem is basically a necessary and sufficient condition for n to be prime, because one can quite easily show that $(n-1)! \equiv 0 (\mathrm{mod}\, n)$ when $n > 4$ is composite. However, it is not practically useful as a primality test.

CHAPTER 3

Primitive roots and the structure of $(\mathbb{Z}/q\mathbb{Z})^\times$

3.1. The group $(\mathbb{Z}/q\mathbb{Z})^\times$ and Euler's ϕ-function

We write $(\mathbb{Z}/q\mathbb{Z})^\times$ for the set of elements of $\mathbb{Z}/q\mathbb{Z}$ which have multiplicative inverses. This is a group under multiplication (but not under addition).

DEFINITION 3.1 (Euler's ϕ-function). We define $\phi(n)$ to be the number of positive integers less than or equal to n and coprime to n.

LEMMA 3.1. *We have* $\#(\mathbb{Z}/q\mathbb{Z})^\times = \phi(q)$.

Proof. Every element of $\mathbb{Z}/q\mathbb{Z}$ is congruent to precisely one element of $\{1, \dots, q\}$, and the elements of $(\mathbb{Z}/q\mathbb{Z})^\times$ correspond to the elements of this set which are coprime to q. □

PROPOSITION 3.1. *Suppose that $q_1, \dots, q_k$ are pairwise coprime positive integers. Then*

$$(\mathbb{Z}/q_1\mathbb{Z})^\times \times \cdots (\mathbb{Z}/q_k\mathbb{Z})^\times \cong (\mathbb{Z}/q_1 \dots q_k\mathbb{Z})^\times$$

as groups.

Proof. The proof of the Chinese remainder theorem adapts almost immediately to give this. Consider once again the map

$$\psi : \mathbb{Z}/q_1 \cdots q_k\mathbb{Z} \to \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_k\mathbb{Z}$$

given by

$$\psi(x + q_1 \cdots q_k\mathbb{Z}) = (x + q_1\mathbb{Z}, \dots, x + q_k\mathbb{Z}).$$

Note that the image of $(\mathbb{Z}/q_1 \cdots q_k\mathbb{Z})^\times$ is precisely $(\mathbb{Z}/q_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/q_k\mathbb{Z})^\times$, since x is coprime to $q_1 \cdots q_k$ if and only if it is coprime to each q_i. We have already shown, in the proof of the Chinese Remainder Theorem, that ψ is a bijection, and so it is also a bijection when restricted to $(\mathbb{Z}/q_1 \cdots q_k\mathbb{Z})^\times$. Since ψ is a ring homomorphism (and hence respects multiplication), it restricts to a group homomorphism on $(\mathbb{Z}/q_1 \cdots q_k\mathbb{Z})^\times$. Since this homomorphism is bijective onto its image, it is in fact an isomorphism. □

COROLLARY 3.1. *The ϕ-function is multiplicative, that is to say $\phi(mn) = \phi(m)\phi(n)$ if $(m,n) = 1$.*

Proof. Simply apply Proposition 3.1 with $m = q_1$ and $n = q_2$. □

COROLLARY 3.2. *Suppose that n is a positive integer and that its prime factorisation is $p_1^{a_1} \cdots p_k^{a_k}$. Then*

$$\phi(n) = p_1^{a_1-1}(p_1 - 1) \cdots p_k^{a_k-1}(p_k - 1) = n \prod_{p|n} (1 - \frac{1}{p}).$$

Proof. Follows immediately from the preceding corollary and the observation that $\phi(p^a) = p^{a-1}(p-1)$, this being the number of integers $\leqslant p^a$ which are not multiples of p. □

3.2. The Fermat–Euler theorem

Fermat's Little Theorem can be generalised to composite q, with an almost identical proof.

THEOREM 3.1 (Fermat–Euler). *Suppose that q is a positive integer, and that a is coprime to q. Then $a^{\phi(q)} \equiv 1 (\mathrm{mod}\, q)$.*

Proof. Let $x_1, \ldots, x_{\phi(q)}$ be a complete set of residues coprime to q: that is, a set of integers, mutually incongruent modulo q, and each coprime to q. Equivalently, the $x_i + q\mathbb{Z}$ are precisely the elements of $(\mathbb{Z}/q\mathbb{Z})^\times$. Consider the integers $ax_1, \ldots, ax_{\phi(q)}$. Each of these is coprime to q and these integers are multually incongruent modulo q; if $ax_i \equiv ax_j (\mathrm{mod}\, q)$ then $q | a(x_i - x_j)$, and so $q | x_i - x_j$. Note that here we used Lemma 1.1 (ii) and (iv). Therefore $ax_1, \ldots, ax_{\phi(q)}$ is also a complete set of residues coprime to q.

Taking products gives

$$\prod_{i=1}^{\phi(q)} x_i \equiv \prod_{i=1}^{\phi(q)} (ax_i) \equiv a^{\phi(q)} \prod_{i=1}^{\phi(q)} x_i (\mathrm{mod}\, q).$$

By the cancellation lemma, the result follows. □

3.3. The order of an element

Suppose that q is a positive integer and that a is an integer coprime to q. Then the order $\mathrm{ord}_q(a)$ is defined to be the smallest positive integer n such that $a^n \equiv 1 (\mathrm{mod}\, q)$.

Note that $\mathrm{ord}_q(a)$ depends only on $a (\mathrm{mod}\, q)$, and so we can define ord_q as a function on $(\mathbb{Z}/q\mathbb{Z})^\times$.

For example, we have $\mathrm{ord}_7(2) = 3$, because $2^3 \equiv 1 (\mathrm{mod}\, 7)$, but neither 2 nor 2^2 is $\equiv 1 (\mathrm{mod}\, 7)$.

Here is the most basic property of the order.

LEMMA 3.2. $\mathrm{ord}_q(a)$ *exists. If* $a^N \equiv 1 (\mathrm{mod}\, q)$ *then* $\mathrm{ord}_q(a) | N$. *In particular,* $\mathrm{ord}_q(a) | \phi(q)$.

Proof. Existence follows immediately from the Fermat–Euler theorem. Suppose now that $n = \mathrm{ord}_a(q)$, and write $N = mn + r$ where $0 \leqslant r < n$. Since $a^n \equiv 1 (\mathrm{mod}\, q)$, we have $a^r \equiv (a^n)^m a^r = a^{mn+r} = a^N \equiv 1 (\mathrm{mod}\, q)$. However, n is supposed to be the *least* positive integer with $a^n \equiv 1 (\mathrm{mod}\, q)$, we must have $r = 0$. This implies that $n | N$. The last part follows from the Fermat-Euler theorem. □

We remark that the converse also holds, since if $n = \mathrm{ord}_q(a)$ and $n | N$ then

$$a^N \equiv (a^n)^{N/n} \equiv 1 (\mathrm{mod}\, q).$$

These statements are in fact consequences of Lagrange's theorem in group theory, which states that if H is a subgroup of a group G then $\#H | \#G$. Here, we apply this with $G = (\mathbb{Z}/q\mathbb{Z})^\times$ and with H the subgroup generated by a, which has $\#H = \mathrm{ord}_q(a)$.

We conclude with another simple property of the order.

LEMMA 3.3. *Suppose that* $\mathrm{ord}_q(a_1) = n_1$ *and* $\mathrm{ord}_q(a_2) = n_2$ *and that* $(n_1, n_2) = 1$. *Then* $\mathrm{ord}_q(a_1 a_2) = n_1 n_2$.

Proof. Let $N := \mathrm{ord}_q(a_1 a_2)$. We have

$$(a_1 a_2)^{n_1 n_2} \equiv (a_1^{n_1})^{n_2} (a_2^{n_2})^{n_1} \equiv 1 (\mathrm{mod}\, q),$$

and so $N | n_1 n_2$ by Lemma 3.2. In the other direction, consider the equation $(a_1 a_2)^N \equiv 1 (\mathrm{mod}\, q)$. Raising both sides to the power n_2 gives $a_1^{N n_2} \equiv 1 (\mathrm{mod}\, q)$ and hence, by Lemma 3.2, $n_1 | N n_2$. Since n_1 and n_2 are coprime, it follows that $n_1 | N$. Similarly $n_2 | N$, and hence (again using the fact that n_1, n_2 are coprime), $n_1 n_2 | N$. □

One of our main aims in this chapter is to prove the following result.

PROPOSITION 3.2. *Let* p *be a prime. Then there is an element* $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ *with* $\mathrm{ord}_p(g) = p - 1$. *Equivalently,* $(\mathbb{Z}/p\mathbb{Z})^\times$ *is a cyclic group.*

Remarks. An element g with this property is called a *primitive root* modulo p. For some reason, use of the letter g in this context is quite common. If a is an integer whose reduction modulo p has this property then we also call g a primitive root modulo p; in fact this usage is more common. If g is a primitive root then,

by definition, a complete list of the elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ is $\{1+p\mathbb{Z}, g+p\mathbb{Z}, g^2+p\mathbb{Z}, \dots, g^{p-2}+p\mathbb{Z}\}$. For example, working mod 11 we have $\{1,2,2^2,2^3,\dots,2^9\} \equiv \{1,2,4,8,5,10,9,7,3,6\}$, so 2 is a primitive root modulo 11. Let us remark in passing that it is an unsolved problem (Artin's Conjecture) whethe 2 is a primitive root for infinitely many primes p.

3.4. Polynomial equations modulo a prime

The results of this section, while not without interest in their own right, are here because we need them to prove Proposition 3.2.

Everyone knows that quadratic equations over $\mathbb{R}$ have at most two roots, and that over $\mathbb{C}$ they have exactly two (counted with multiplicity). In the residue ring $\mathbb{Z}/q\mathbb{Z}$, the analogue of this can fail. For example, in $\mathbb{Z}/8\mathbb{Z}$ the equation $x^2-1=0$ has four distinct solutions, namely $x=1,3,5,7$.

When $q=p$ is prime, things are much better behaved. This is because $\mathbb{Z}/p\mathbb{Z}$ is an integral domain, that is to say a ring with no zero divisors: if $ab=0$ then $a=0$ or $b=0$. (In fact, $\mathbb{Z}/p\mathbb{Z}$ is a field since, as we have shown, all non-zero elements have multiplicative inverses.)

PROPOSITION 3.3. *Let $f(X) \in R[X]$ be a polynomial of degree $d \geqslant 0$ over an integral domain R. Then f has at most d roots in R.*

Proof. If f has no roots we are done, so let's suppose $\alpha \in R$ is a root.

By the division algorithm for polynomials $f(X) = (X-\alpha)q(X)+c$ for some $c \in R$. (See Prelims for polynomials over the reals; the same works for a general integral domain.) Thus $0=(\alpha-\alpha)q(\alpha)+c$ so $c=0$. Now let $\beta \in R$ be any other root of $f(x)$. Then $0=f(\beta)=(\alpha-\beta)q(\beta)$ and since $\alpha-\beta \neq 0$ and R is an integral domain, we deduce that $q(\beta)=0$. But q is a polynomial of degree $d-1$ and so by induction has $\leqslant d-1$ roots. Hence f has at most $1+(d-1)=d$ roots. □

LEMMA 3.4. *Let p be a prime, and suppose that $d|p-1$. Then there are exactly d values of $x \in \mathbb{Z}/p\mathbb{Z}$ such that $x^d \equiv 1 (\mathrm{mod}\, p)$.*

Proof. The polynomial X^d-1 is a factor of $X^{p-1}-1$:

$$X^{p-1}-1 = (X^d-1)g(X)$$

where

$$g(X) = 1 + X^d + X^{2d} + \cdots + X^{(\frac{p-1}{d}-1)d}.$$

By Fermat's Little Theorem, every $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ is a root of the left hand side. By Proposition 3.3, at most $\deg g = p-1-d$ of these can be roots of g. The other d values of x must therefore be roots of X^d-1. By Proposition 3.3, this polynomial cannot have *more* than these d roots. □

3.5. Existence of primitive roots

In this section we give the proof of Proposition 3.2. We first give a lemma that will be used in the proof.

LEMMA 3.5. *Suppose that p is a prime. Let q be another prime and suppose that $q^c | p-1$ for some integer c. Then there is some $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ with $\mathrm{ord}_p(a) = q^c$.*

Proof. By Lemma 3.4, there are q^c values of $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ with $x^{q^c} \equiv 1 (\mathrm{mod}\, p)$. If such an element x does *not* have $\mathrm{ord}_p(x) = q^c$ then, since $\mathrm{ord}_p(x) | q^c$, we must have $\mathrm{ord}_p(x) | q^{c-1}$ and hence $x^{q^{c-1}} \equiv 1 (\mathrm{mod}\, p)$. By Lemma 3.4 again, the number of elements with this property is q^{c-1}. Therefore there are $q^c - q^{c-1} > 0$ elements x with $\mathrm{ord}_p(x) = q^c$. □

Proof. [Proof of Proposition 3.2] Factor $p-1 = q_1^{c_1} \dots q_k^{c_k}$ as a product of primes. By Lemma 3.5, there are elements $a_i \in (\mathbb{Z}/p\mathbb{Z})^\times$ with $\mathrm{ord}_p(a_i) = q_i^{c_i}$. Set $a := a_1 \cdots a_k$. By Lemma 3.3, $\mathrm{ord}_p(a) = q_1^{c_1} \cdots q_k^{c_k} = p-1$. □

3.6. *The structure of $(\mathbb{Z}/q\mathbb{Z})^\times$

I do not regard this section as examinable, but it is material that any number theorist should be familiar with.

First observe that, to understand the structure of $(\mathbb{Z}/q\mathbb{Z})^\times$, it is enough by Proposition 3.1 to understand the case $q = p^r$.

LEMMA 3.6. *Suppose that p is an odd prime. Then $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is cyclic.*

Proof. The case $r = 1$ is Proposition 3.2. Next we handle $r = 2$. Suppose that g is a primitive root modulo p. Let $n := \mathrm{ord}_{p^2}(g)$. Then Lemma 3.2 implies that $n | p(p-1)$. On the other hand, we certainly have $g^n \equiv 1 (\mathrm{mod}\, p)$ and so, since g is a primitive root mod p, $(p-1) | n$. If $n = p(p-1)$, we are done. The only other possibility is that $n = p-1$.

In this case, $g^{p-1} = 1 (\mathrm{mod}\, p^2)$. Consider $\tilde{g} := g + p$. Note that $\tilde{g}$ is still a primitive root modulo p. Then

$$\begin{aligned} \tilde{g}^{p-1} = (g+p)^{p-1} &= g^{p-1} + \binom{p-1}{1} p g^{p-2} + \dots \\ &\equiv g^{p-1} + p(p-1) g^{p-2} (\mathrm{mod}\, p^2) \\ &\equiv 1 + p(p-1) g^{p-2} (\mathrm{mod}\, p^2) \end{aligned}$$

(the dots represent integers divisible by p^2). Evidently $p^2 \nmid p(p-1)g^{p-2}$, and so $\tilde{g}^{p-1} \neq 1 (\mathrm{mod}\, p^2)$.

By the comments in the first paragraph, we must have $\mathrm{ord}_{p^2}(\tilde{g}) = p(p-1)$. This completes the analysis of the case $r = 2$.

We remark that what we did here was essentially to find an appropriate "lift" of a primitive root modulo p to a generator for $(\mathbb{Z}/p^2\mathbb{Z})^\times$; we began by taking an arbitrary lift to $\mathbb{Z}$, and then argued that either this, or this $+p$, works.

We claim that if $\operatorname{ord}_{p^2}(g) = p(p-1)$ then $\operatorname{ord}_{p^r}(g) = p^{r-1}(p-1)$ for all $r \geqslant 2$. Note that if $g^n \equiv 1 (\operatorname{mod} p^r)$ then $g^n \equiv 1 (\operatorname{mod} p^2)$, and so $p(p-1) | \operatorname{ord}_{p^r}(g)$. Also, $\operatorname{ord}_{p^r}(g) | p^{r-1}(p-1)$. Thus $\operatorname{ord}_{p^r}(g) = p^{e(r)}(p-1)$ for some $e(r)$, $1 \leqslant e(r) \leqslant r-1$. We claim that $e(r) = r-1$, to which end it suffices to show that we do not have $e(r) \leqslant r-2$, or in other words that

$$g^{p^{r-2}(p-1)} \neq 1 (\operatorname{mod} p^r). \tag{3.1}$$

We will prove this by induction on r, the case $r = 2$ having already been established.

Suppose that we know (3.1) for some $r \geqslant 2$. Then, since $g^{p^{r-2}(p-1)} \equiv 1 (\operatorname{mod} p^{r-1})$, we have

$$g^{p^{r-2}(p-1)} = 1 + tp^{r-1}$$

for some t with $p \nmid t$. Then

$$\begin{aligned} g^{p^{r-1}(p-1)} &= (1 + tp^{r-1})^p \\ &= 1 + tp^r + \binom{p}{2} t^2 p^{2(r-1)} + \dots \end{aligned}$$

by the binomial theorem. Note that $1 + tp^r \neq 1 (\operatorname{mod} p^{r+1})$. We claim that all further terms are divisible by p^{r+1}. The term $\binom{p}{2} t^2 p^{2(r-1)}$ is divisible by p^{2r-1}, since $p | \binom{p}{2}$ (here we used the fact that $p \neq 2$). When $r \geqslant 2$, $2r - 1 \geqslant r + 1$. Each subsequent term is divisible by $p^{3(r-1)}$. When $r \geqslant 2$, $3(r-1) \geqslant r+1$.

This establishes the claim, and it follows that (3.1) also holds for $r+1$. This concludes the proof. □

Note that we made crucial use of the fact that $p \neq 2$ in the above, at the point where we noted that $p | \binom{p}{2}$. This is not true when $p = 2$, and indeed the situation is different in that case. We have $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$ and $(\mathbb{Z}/4\mathbb{Z})^\times = \{1, 3\}$, isomorphic to the cyclic group C_2. However, the groups $(\mathbb{Z}/2^r\mathbb{Z})^\times$, $r \geqslant 3$, are *not* cyclic.

LEMMA 3.7. *The group $(\mathbb{Z}/2^k\mathbb{Z})^\times$ is isomorphic to $C_2 \times C_{2^{k-2}}$.*

Proof. We first claim that

$$\operatorname{ord}_{2^k}(5) = 2^{k-2}. \tag{3.2}$$

To prove this, we must show that $5^{2^{k-3}} \neq 1 (\operatorname{mod} 2^k)$, to which end we use the binomial theorem and the fact that $5 = 2^2 + 1$ to compute that

$$5^{2^{k-3}} = (2^2 + 1)^{2^{k-3}} = 1 + 2^{k-1} + \sum_{i \geqslant 2} \binom{2^{k-3}}{i} 2^{2i}.$$

We claim that this is $\equiv 1+2^{k-1} (\mathrm{mod}\, 2^k)$, and hence certainly not $\equiv 1 (\mathrm{mod}\, 2^k)$. To show this, it suffices to show that each of the terms in the sum over i is divisible by 2^k. Writing $\nu_2(n)$ for the highest exponent of a power of two dividing n, we must show that

$$\nu_2\Big(\binom{2^{k-3}}{i}\Big) \geqslant k-2i. \tag{3.3}$$

Now $\binom{2^{k-3}}{i} = \frac{2^{k-3}}{i}\binom{2^{k-3}-1}{i-1}$, and so

$$\nu_2\Big(\binom{2^{k-3}}{i}\Big) \geqslant k-3-\nu_2(i).$$

Thus (3.3) follows if we can show that

$$2i \geqslant \nu_2(i)+3. \tag{3.4}$$

This is trivially checked when $i=2$, and for $i \geqslant 3$ we may use the very crude inequality $\nu_2(i) < i$, which follows from the fact that $2^i > i$. Thus (3.4) holds, and hence so does (3.3) and the claim (3.2).

Let $\langle 5\rangle \leqslant (\mathbb{Z}/2^k\mathbb{Z})^\times$ be the group generated by 5, thus

$$\langle 5\rangle = \{1, 5, 5^2, \dots, 5^{2^{k-2}-1}\}.$$

We proved above that $5^{2^{k-3}} \equiv 1+2^{k-1} (\mathrm{mod}\, 2^k)$. Note that this is *not* $-1 (\mathrm{mod}\, 2^k)$, and hence in fact -1 does not lie in $\langle 5\rangle$: if $-1 = 5^n (\mathrm{mod}\, 2^k)$ then $1 = 5^{2n} (\mathrm{mod}\, 2^k)$ and so $2n | \operatorname{ord}_{2^k}(5) = 2^{k-2}$, and hence $n | 2^{k-3}$. It follows that the elements $(-1)^e 5^j$, $e = 0, 1$, $j = 0, 1, \dots, 2^{k-2}-1$, are all distinct. Since there are 2^{k-1} of these elements we have

$$(\mathbb{Z}/2^k\mathbb{Z})^\times \cong \{\pm 1\} \times \langle 5\rangle.$$

□

Finally, we can characterise all q for which there is a primitive root $(\mathrm{mod}\, q)$, that is to say for which $(\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic.

PROPOSITION 3.4. *$(\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic if and only if q is $2, 4$, an odd prime power or twice an odd prime power.*

Proof. We use two facts from group theory: first, that a product $G = C_{n_1} \times \cdots \times C_{n_r}$ is not cyclic unless $n_1, \dots, n_r$ are coprime. (In fact this is an if and only if, but the direction we need is rather easy: every element in this group has order dividing the lowest common multiple $[n_1, \dots, n_r]$, which is strictly smaller than $\#G$.) The second fact from group theory that we shall use is that every subgroup of a cyclic group is cyclic (note that the proof of this is extremely similar to the proof of Lemma 3.2).

Suppose first that q has two odd prime factors p_1, p_2. Then $(\mathbb{Z}/q\mathbb{Z})^\times$ is a product of cyclic groups, two of which have orders $p_1^{a_1-1}(p_1-1)$ and $p_2^{a_2-1}(p_2-1)$, both of which are even. Thus $(\mathbb{Z}/q\mathbb{Z})^\times$ is not cyclic in this case.

If q is divisible by 8 then it has a non-cyclic subgroup $(\mathbb{Z}/2^k\mathbb{Z})^\times$, and so is not cyclic by the second group theory fact.

If q is divisible by 4 and an odd prime then it has a subgroup $C_2 \times (\mathbb{Z}/p^a\mathbb{Z})^\times$, a product of cyclic groups, both of even order.

In all other cases, $(\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic by inspection. □

CHAPTER 4

Quadratic Residues and reciprocity

4.1. Quadratic residues. Euler's criterion

Let p be an odd prime, and let $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. We say that a is a *quadratic residue* if there is some integer x such that $x^2 = a (\mathrm{mod}\, p)$, and a *quadratic nonresidue* otherwise.

LEMMA 4.1. *There are exactly* $(p-1)/2$ *quadratic residues and exactly* $(p-1)/2$ *quadratic nonresidues.*

Proof. The map $x \mapsto x^2$ is 2–1 on $(\mathbb{Z}/p\mathbb{Z})^\times$, because x and y map to the same point if and only if $x \equiv -y$. The image of this map is precisely the set of quadratic residues. □

LEMMA 4.2. *We have the following statements.*

(i) *The product of two quadratic residues is a quadratic residue;*
(ii) *The product of a quadratic residue and a quadratic nonresidue is a quadratic nonresidue;*
(iii) *The product of two quadratic nonresidues is a quadratic residue.*

Proof. All of this follows from the observation that the quadratic residues are a subgroup G of $(\mathbb{Z}/p\mathbb{Z})^\times$ of index 2. That they are a subgroup (closed under products and inverses) is easily checked, in in fact this already confirms (i). That they have index 2 follows from Lemma 4.1.

Since $(\mathbb{Z}/p\mathbb{Z})^\times$ is abelian, G is normal and hence there is a quotient homomorphism $\psi : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times/G$, where the right-hand side is a group of order 2. Of course this group is unique up to isomorphism, and it is traditional to identify it with $\{-1, 1\} \subset \mathbb{R}$, with the group operation being multiplication.

To spell it out, there is a (unique!) map $\psi : (\mathbb{Z}/p\mathbb{Z})^\times \to \{-1, 1\}$ such that $\psi(ab) = \psi(a)\psi(b)$ and such that a is a quadratic residue if and only if $\psi(a) = 1$. □

Note that the statement of this lemma is very concrete and, if you have trouble thinking about quotient groups, you need not worry yourself any further. Moreover, here is a sketch of a more hands-on proof. First note that (i) and (ii) are true almost straight from the definition. For example if a_1, a_2 are quadratic residues

and a_3 is a nonresidue then we cannot have $a_1a_3 = a_2$, since $a_2a_1^{-1}$ is a quadratic residue. Now fix some nonresidue a. The set $\{ax : x \text{ a quadratic residue}\}$ has size $(p-1)/2$ and consists entirely of quadratic nonresidues, by (ii). Therefore the set $\{ax : x \text{ a quadratic nonresidue}\}$, which is the complement of the preceding set, is precisely the set of quadratic residues.

PROPOSITION 4.1 (Euler's criterion). *Let p be an odd prime, and suppose that $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Then*

$$a^{(p-1)/2} \equiv \begin{cases} 1 (\mathrm{mod}\, p) & \text{if } a \text{ is a quadratic residue } (\mathrm{mod}\, p) \\ -1 (\mathrm{mod}\, p) & \text{if } a \text{ is a quadratic nonresidue } (\mathrm{mod}\, p). \end{cases}$$

Proof. By Fermat's Little Theorem, $(a^{(p-1)/2})^2 \equiv 1 (\mathrm{mod}\, p)$, and hence $a^{(p-1)/2} \equiv \pm 1 (\mathrm{mod}\, p)$. Since an equation of degree $d < p$ has at most d roots, there are at most $(p-1)/2$ values of a satisfying each of these two conditions. Since all $p-1$ values of $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ satisfy *one* of these conditions, there must be exactly $(p-1)/2$ values of a with $a^{(p-1)/2} \equiv 1 (\mathrm{mod}\, p)$, and exactly $(p-1)/2$ values of a with $a^{(p-1)/2} \equiv -1 (\mathrm{mod}\, p)$.

Suppose that a is a quadratic residue. Then $a \equiv x^2 (\mathrm{mod}\, p)$ for some x, and hence $a^{(p-1)/2} \equiv x^{p-1} \equiv 1 (\mathrm{mod}\, p)$, by Fermat's Little Theorem. Therefore the $(p-1)/2$ quadratic residues are precisely the $(p-1)/2$ values of a for which $a^{(p-1)/2} \equiv 1 (\mathrm{mod}\, p)$. □

Remark. In the notation of the proof of Lemma 4.2, we have

$$\psi(a) \equiv a^{(p-1)/2} (\mathrm{mod}\, p).$$

Note that the proof of Euler's criterion made no use of Lemma 4.2. Therefore, since it is obvious that $(ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} (\mathrm{mod}\, p)$, it may used to give yet another proof of that lemma.

Here is a simply corollary of Euler's criterion.

COROLLARY 4.1. *Let p be an odd prime. Then -1 is a quadratic residue mod p if and only if $p \equiv 1 (\mathrm{mod}\, 4)$.*

Proof. Immediate from Euler's criterion. □

4.2. The Legendre symbol. Statement of the reciprocity law

Suppose that p is a prime, and now let $a \in \mathbb{Z}$. We define the *Legendre symbol* $\left(\frac{a}{p}\right)$ to equal 1 if $(a,p) = 1$ and if $a (\mathrm{mod}\, p)$ is a quadratic residue modulo p, -1 if $(a,p) = 1$ and if $a (\mathrm{mod}\, p)$ is a quadratic nonresidue modulo p, and 0 if $p|a$.

For example, $\left(\frac{23}{7}\right) = 1$ because $23 \equiv 4^2 (\mathrm{mod}\, 7)$.

LEMMA 4.3. *The Legendre symbol enjoys the following basic properties.*

(i) $\left(\frac{1}{p}\right) = 1$;

(ii) $\left(\frac{a+kp}{p}\right) = \left(\frac{a}{p}\right)$ *for any* $k \in \mathbb{Z}$;

(iii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Proof. We have basically proved all of this already. Part (i) is obvious because $1 = 1^2$. Part (ii) follows immediately from the definition of the Legendre symbol, which only cares about the value of a *modulo* p. Finally, (iii) is a consequence of Lemma 4.2 when a and b are coprime to p. If one of a, b is divisible by p then both sides of (iii) are zero. □

The main aim of this chapter is to prove the following remarkable and famous result of Gauss, called the Law of Quadratic Reciprocity.

THEOREM 4.1. *Let* p, q *be distinct odd primes. We have*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} -1 & \text{if } p \equiv q \equiv 3 (\mathrm{mod}\, 4) \\ 1 & \text{otherwise} \end{cases}$$

We remark that a more succinct way to write this is

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4},$$

and this is how you will often see the formula written in books.

We will also establish the following statement about the quadratic nature of 2 modulo an odd prime.

PROPOSITION 4.2. *The number* 2 *is a quadratic residue* $(\mathrm{mod}\, p)$ *if and only if* $p \equiv \pm 1 (\mathrm{mod}\, 8)$.

The reciprocity law (Theorem 4.1), Proposition 4.2 and more elementary facts about the Legendre symbol presented in Lemma 4.3 give a usable algorithm for evaluating the Legendre symbol in practice. Rather than describe this formally in generality, we give an illustrative example.

EXAMPLE 4.1. Is 101 a quadratic residue modulo 163?

First note that 101 and 163 are both prime, and that not both of them are $3 (\mathrm{mod}\, 4)$. Therefore $\left(\frac{101}{163}\right) = \left(\frac{163}{101}\right)$. Reducing 163 modulo 101 shows that this equals $\left(\frac{62}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{31}{101}\right)$. We know that $\left(\frac{2}{101}\right) = -1$, since $101 \equiv 5 (\mathrm{mod}\, 8)$. To evaluate $\left(\frac{31}{101}\right)$, we use reciprocity again to see that it equals $\left(\frac{101}{31}\right)$. Since $101 \equiv 8 (\mathrm{mod}\, 31)$, this is $\left(\frac{8}{31}\right)$, which equals $\left(\frac{2}{31}\right)^3 = \left(\frac{2}{31}\right)$, which equals 1 since $31 \equiv 7 (\mathrm{mod}\, 8)$. Putting all this together gives $\left(\frac{101}{163}\right) = -1$, and so 101 is not a quadratic residue modulo 163.

4.3. Gauss's lemma

In this section we present Gauss's lemma, from which Proposition 4.2 follows quite easily, and which is the key technical ingredient in the proof of the reciprocity law.

PROPOSITION 4.3 (Gauss's Lemma). *Let p be an odd prime. Let $I \subset (\mathbb{Z}/p\mathbb{Z})^\times$ be a set such that $(\mathbb{Z}/p\mathbb{Z})^\times$ is the disjoint union of I and $-I = \{-i : i \in I\}$. Let a be an integer coprime to p. Then $\left(\frac{a}{p}\right) = (-1)^t$, where $t = \#\{j \in I : aj \in -I\}$.*

Proof. Write

$$J_- := \{j \in I : aj \in -I\}$$

and

$$J_+ := \{j \in I : aj \in I\}.$$

Then J_-, J_+ are disjoint and their union is I .

We claim that $-aJ_-$ and aJ_+ (where $aX := \{ax : x \in X\}$) are disjoint and that *their* union is I. They are disjoint because $-aj_- \equiv aj_+$ implies $-j_- \equiv j_+$, which is impossible since I and $-I$ are disjoint. From the definitions, $-aJ_-$ and aJ_+ are both contained in I. Therefore the claim follows by computing cardinalities:

$$\#(-aJ_- \cup aJ_+) = \#J_- + \#J_+ = \#(J_- \cup J_+) = \#I.$$

Thus the product of the elements of I, modulo p, is

$$\begin{aligned}\prod_{j\in J_-}(-aj_-)\cdot\prod_{j\in J_+}(aj_+) &\equiv a^{(p-1)/2}(-1)^{\#J_-}\prod_{j\in J_-\cup J_+} j\\ &\equiv a^{(p-1)/2}(-1)^{\#J_-}\prod_{j\in I} j.\end{aligned}$$

Cancelling $\prod_{j\in I} j$ (which is coprime to p) gives

$$a^{(p-1)/2}(-1)^{\#J_-} \equiv 1 (\mathrm{mod}\, p),$$

and so

$$a^{(p-1)/2} \equiv (-1)^{\#J_-}.$$

The result now follows immediately from Euler's criterion. □

We remark that Gauss's lemma is invariably applied with

$$I := \{1, \ldots, (p-1)/2\},$$

considered as a subset of $\mathbb{Z}/p\mathbb{Z}$ (by a slight abuse of notation). When we speak of "Gauss's lemma" we will assume that this choice of I has been made, but we wanted to illustrate the fact that the proof makes little use of the specific choice.

Using Gauss's lemma, we prove Proposition 4.2.

Proof. We compute the parity of

$$t = \#\{j \in I : 2j \in -I\},$$

where $I = \{1, \dots, (p-1)/2\}$. Write $p = 8k + 2r + 1$, $r \in \{0, 1, 2, 3\}$, so that

$$I = \{1, \dots, 4k + r\}$$

and

$$-I = \{4k + r + 1, \dots, 8k + 2r\}.$$

The elements $j \in I$ with $2j \in -I$ are precisely

$$2k + r', \dots, 4k + r,$$

where r' is the least integer with $2r' \geqslant r + 1$. The quantity t is the parity of the number of these elements, which is the same as the parity of $u := \#\{r', \dots, r + 2\}$ (by adding/removing an even number of elements from each end of the interval). Splitting into cases, we see that

- When $r = 0$, $r' = 1$, $u = 2$;
- When $r = 1$, $r' = 1$, $u = 3$;
- When $r = 2$, $r' = 2$, $u = 3$;
- When $r = 3$, $r' = 2$, $u = 4$.

The result follows. □

4.4. Proof of the reciprocity law

In this section we prove Theorem 4.1.

Proof. Let

$$E = \{(x, y) \subset \mathbb{Z}^2 : 1 \leqslant x \leqslant \frac{1}{2}(p-1), 1 \leqslant y \leqslant \frac{1}{2}(q-1)\}.$$

Divide E into the following four sets:

$$E_1 := \{(x, y) \in E : qx - py < -\frac{p}{2}\},$$

$$E_2 := \{(x, y) \in E : -\frac{p}{2} < qx - py < 0\},$$

$$E_3 := \{(x, y) \in E : 0 < qx - py < \frac{q}{2}$$

and

$$E_4 := \{(x, y) \in E : qx - py > \frac{q}{2}\}.$$

Obviously these sets are disjoint, and they do cover E since $qx - py$ is never 0 for $(x, y) \in E$, and neither $-\frac{p}{2}$ nor $\frac{q}{2}$ is an integer.

Write $t_i := \#E_i$.

We claim that

$$\left(\frac{q}{p}\right) = (-1)^{t_2}.$$

To see this, we use Gauss's lemma, which tells us that $\left(\frac{q}{p}\right) = (-1)^t$ where

$$\begin{aligned} t &= \#\{x \in \{1, \dots, \frac{1}{2}(p-1)\} : qx \in \{-\frac{1}{2}(p-1), \dots, -1\} (\mathrm{mod}\, p)\}. \\ &= \#\{x \in \{1, \dots, \frac{1}{2}(p-1)\} : \exists y \in \mathbb{Z}, -\frac{p}{2} < qx - py < 0\}. \end{aligned}$$

The value of y is unique. Moreover if $y \leqslant 0$ then $qx - py > 0$, whilst if $y \geqslant \frac{1}{2}(q+1)$ then $qx - py \leqslant \frac{1}{2}q(p-1) - \frac{1}{2}p(q+1) < -\frac{p}{2}$, so $y \in \{1, \dots, \frac{1}{2}(q-1)\}$. Thus we in fact have $t = t_2$, thereby confirming the claim.

By a completely symmetric argument,

$$\left(\frac{p}{q}\right) = (-1)^{t_3}.$$

We claim that $t_1 = t_4$. To see this, one notes that the map $(x, y) \mapsto (\frac{1}{2}(p+1) - x, \frac{1}{2}(q+1) - y)$ is a bijection between these two sets. The proof is an easy calculation: if $x' = \frac{1}{2}(p+1) - x$ and $y' = \frac{1}{2}(q+1) - y$ then

$$\begin{aligned} & qx - py < -\frac{p}{2} \\ \iff \quad & q\big(\frac{1}{2}(p+1) - x'\big) - p\big(\frac{1}{2}(q+1) - y'\big) < -\frac{p}{2} \\ \iff \quad & -qx' + py' < -\frac{q}{2} \\ \iff \quad & qx' - py' > \frac{q}{2}. \end{aligned}$$

Putting all this together gives

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{t_2+t_3} = (-1)^{t_1+t_2+t_3+t_4} = (-1)^{\#E} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

This concludes the proof. □

CHAPTER 5

Factorisation and primality testing

5.1. Introduction

This is a very brief chapter on an interesting topic, about which much can be said. I recommend the superb book *Prime numbers: a computational perspective* by Crandall and Pomerance for more information. The basic point of this chapter is that

- (we think) it is computationally hard to determine the factors of n, in general;
- it is relatively easy to decide whether or not n is prime (but without finding its factors).

We are not going to delve too deeply into the question of what "hard" and "easy" mean in this context, but they are measured in terms of the number of binary digits of n, which is roughly $\log_2 n$: this is the amount of space required to store n on a computer.

Apropos the second point above, the following famous theorem was established in 2005.

THEOREM 5.1 (Agrawal, Kayal, Saxena). *There is an algorithm to determine whether or not n is prime in time polynomial in* $\log n$.

We will not describe this algorithm (though it is not extraordinarily difficult to do so). We will describe an algorithm that, for practical purposes, is just as good. By contrast the following is an unsolved problem.

QUESTION 5.1. Is there a polynomial time algorithm to find a factor of n?

It is widely suspected that the answer is no, but low bounds for the running times of possible algorithms are notoriously hard to come by. (Indeed this is basically the P vs NP problem, although the factorisation problem itself is not central when those issues are discussed, because it is suspected not to be NP-complete.)

5.2. Trial division and Fermat's method

A very simple observation is that, to find a prime factor of n or prove that none exists, we need only try dividing n by the primes less than or equal to $\sqrt{n}$. Indeed

if d is a divisor of n then so is n/d, and one of these numbers is $\leqslant \sqrt{n}$. Thus of n has a divisor (other than 1 or n) then it has a divisor of size $\leqslant \sqrt{n}$, and hence a prime factor $p \leqslant \sqrt{n}$.

This is very effective for small n (for $n \leqslant 400$ one need only test for divisibility by $2, 3, 5, 7, 11, 13, 17, 19$, and one could even commit to memory the "hard" numbers $169, 289, 361, 221, 247, 323$, which means one need only test for divisibility by $2, 3, 5, 7, 11$). For large n this is a terribly inefficient procedure, even on a computer.

Fermat's method. This is a reasonable method for finding the prime factors of four digit numbers by hand, especially if one has a remembered a list of the 4-digit squares. First, remove all the multiples of 2 from the number to be factored. Given an odd number n, let m be the least integer $\geqslant \sqrt{n}$. Now test $m^2 - n$, $(m+1)^2 - n$, $(m+2)^2 - n$ in turn until we find a j such that $(m+j)^2 - n$ is a square, x^2. Then

$$n = (m+j)^2 - x^2 = (m+j-x)(m+j+x).$$

If $n = ab$ (with a and b odd, and $a \leqslant b$ without loss of generality) then this procedure will find a and b, with $j = \frac{1}{2}(a+b) - m$ and $x = \frac{1}{2}(b-a)$. (Note that $m + j = \frac{1}{2}(a+b)$, which is $\geqslant \sqrt{n}$ and hence $\geqslant m$ by the AM–GM inequality $\frac{1}{2}(a+b) \geqslant \sqrt{ab}$, and so $j \geqslant 0$.)

The procedure will be quite efficient if $a \approx b$, but not if a is tiny and b is very large. For the practical factoring of 4-digit numbers by hand, trial division for primes $p \leqslant 19$ (say) followed by the Fermat method if that is unsuccessful is a sensible way to proceed.

EXAMPLE 5.1. Take $n = 6077$. Then $77 < \sqrt{6077} < 78$ so we start to look at $m = 78$, finding:

$$\begin{aligned} 78^2 - 6077 &= 7, \\ 79^2 - 6077 &= 164, \\ 80^2 - 6077 &= 323, \\ 81^2 - 6077 &= 484 = 22^2. \end{aligned}$$

Therefore $6077 = 81^2 - 22^2 = 103 \times 59$.

In lectures, we looked at $n = 8927$. Another example you might care to try is $n = 3869$.

5.3. *More sophisticated methods and running times

Both trial division and the Fermat method run in exponential time (that is, exponential in $\log_2 n$) in the worst cases. Subexponential-time factoring algorithms are known. The first was the continued fraction algorithm. Nowadays many others

are known, going by the names of the quadratic sieve, the number field sieve, and the elliptic curve method.

We will give just a hint of how the first of these works, since it may be described as a refinement of the Fermat method.

Let us try to factor $n = 1649$ using Fermat's method. Then $40 < \sqrt{1649} < 41$, and so we look at

$$\begin{aligned} 41^2 - 1649 &= 32 &&= 2^5, \\ 42^2 - 1649 &= 115 &&= 5 \cdot 23, \\ 43^2 - 1649 &= 200 &&= 2^3 5^2. \end{aligned}$$

None of these is a square, and so Fermat's method has not worked, at least after only three steps (in fact one needs 17 steps to make it work).

Observe, however, that $32 \times 200 = 2^8 \cdot 5^2 = 80^2$. It follows that $(41 \times 43)^2 \equiv 80^2 (\mathrm{mod}\, n)$. Noting that $41 \times 43 \equiv 114 (\mathrm{mod}\, 1649)$, it follows that

$$n | (114 - 80)(114 + 80) = 2 \times 17 \times 2 \times 97.$$

We have uncovered the factorisation of n, namely 17×97.

Of course, it was rather lucky to simply notice that 32×200 was a square. Can we be more sophisticated? One feature of 32 and 200 is that they have only small prime factors. It ought to be easier to multiply together numbers with only small prime factors to give a square.

Indeed, if we have numbers

$$\begin{aligned} x_1 &= p_1^{a_{11}} \cdots p_k^{a_{1k}} \\ &\vdots \\ x_r &= p_1^{a_{r1}} \cdots p_k^{a_{rk}} \end{aligned}$$

Then the problem of a subset of the x_i whose product is a square is equivalent to finding $\varepsilon_i \in \{0, 1\}$ such that $x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}$ is a square, or equivalently

$$(\varepsilon_1, \ldots, \varepsilon_r) \begin{pmatrix} a_{11} & \ldots & a_{1k} \\ \vdots & & \vdots \\ a_{r1} & \ldots & a_{rk} \end{pmatrix}$$

has even entries. This may be viewed as a linear algebra problem $(\mathrm{mod}\, 2)$, or more accurately over the field $\mathbb{F}_2$ with two elements. Standard linear algebra techniques such as Gaussian elimination are then available.

In our example we had $r = 3$, with $x_1 = 32 = 2^5$, $x_2 = 115 = 5 \cdot 23$ and $x_3 = 200 = 2^3 \cdot 5^2$. There are three primes in play, namely $p_1 = 2$, $p_2 = 5$ and $p_3 = 23$. The linear algebra problem to be solved is then

$$(\varepsilon_1, \varepsilon_2, \varepsilon_3) \begin{pmatrix} 5 & 0 & 0 \\ 0 & 1 & 1 \\ 3 & 2 & 0 \end{pmatrix} \equiv 0 (\mathrm{mod}\, 2).$$

We were easily able to find the solution $\varepsilon_1 = \varepsilon_3 = 1$, $\varepsilon_2 = 0$ by inspection, but had this not been the case (or for a larger problem) we could have used more sophisticated methods of linear algebra.

5.4. *The Miller–Rabin test

In this section we describe an efficient method for determining whether or not a number n is prime. We will only describe the method when $n \equiv 3 (\mathrm{mod}\, 4)$, in which case the description and analysis are rather easier than when $n \equiv 1 (\mathrm{mod}\, 4)$. (If you are interested in reading up on the latter, see the book by Crandall and Pomerance mentioned earlier, or for example *The Miller–Rabin Test* by K. Conrad, http://www.math.uconn.edu/∼kconrad/blurbs/ugradnumthy/millerrabin.pdf.

Proposition 5.1. *Suppose that $n \equiv 3 (\mathrm{mod}\, 4)$. Then n is prime if and only if the following is true: for every $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, $a^{(n-1)/2} \equiv \pm 1 (\mathrm{mod}\, n)$.*

Proof. We have already shown the "only if" direction in proving Euler's criterion. (This bit does not use the fact that $n \equiv 3 (\mathrm{mod}\, 4)$.) Conversely, we must show that if $n \equiv 3 (\mathrm{mod}\, 4)$ is composite then there is some $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ with $a^{(n-1)/2} \not\equiv 1 (\mathrm{mod}\, n)$.

Suppose first that $n = p^k$ is a prime power, $k \geqslant 2$. Consider $a = 1 + p$. Then

$$a^{(n-1)/2} = 1 + p\frac{n-1}{2} + p^2 m$$

for some integer m, by the binomial theorem. This certainly cannot be $-1 (\mathrm{mod}\, p^k)$ (it's not even $-1 (\mathrm{mod}\, p)$). It is also not $1 (\mathrm{mod}\, p^k)$ since, though $a^{(n-1)/2} - 1$ is divisible by p, it is not divisible by p^2.

Now suppose that n is not a prime power, say $n = p^k n'$ with $(n', p) = 1$. By the Chinese remainder theorem, there is a with $a \equiv -1 (\mathrm{mod}\, p^k)$ and $a \equiv 1 (\mathrm{mod}\, n')$. But then $a^{(n-1)/2} \equiv -1 (\mathrm{mod}\, p^k)$ (since $(n-1)/2$ is odd) and $a^{(n-1)/2} \equiv 1 (\mathrm{mod}\, n')$. Thus $a^{(n-1)/2} \not\equiv \pm 1 (\mathrm{mod}\, n')$, because $-1 \not\equiv 1 (\mathrm{mod}\, n')$ and $-1 \not\equiv 1 (\mathrm{mod}\, p^k)$. □

Thus, to prove that n is composite, we need only find a "witness": a value of a such that $a^{(n-1)/2} \not\equiv \pm 1 (\mathrm{mod}\, n)$. At first sight, this could be quite hard. However, a simple observation reveals that at least half of all a are witnesses.

LEMMA 5.1. *Suppose that $n \equiv 3 (\mathrm{mod}\, 4)$ and that n is composite. Then the set S of all a with $a^{(n-1)/2} \equiv \pm 1 (\mathrm{mod}\, n)$ is a proper subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Proof. It is obvious that S is closed under multiplication and taking inverses and hence is a subgroup. That it is a *proper* subgroup follows from Proposition 5.1. □

In practice, one now tests for primality of $n \equiv 3 (\mathrm{mod}\, 4)$ by picking $a_1, \dots, a_k \in \{1, \dots, n-1\}$ at random. If some a_i has a factor in common with n then we immediately see that n is composite; otherwise, the a_i are random elements of $(\mathbb{Z}/n\mathbb{Z})^\times$, and so if $a_j^{(n-1)/2} \equiv \pm 1 (\mathrm{mod}\, n)$ for $j = 1, \dots, k$, then one can assert that "n is prime with probability $1 - 2^{-k}$".

For a rigorous result, one must show that $a^{(n-1)/2} \equiv \pm 1 (\mathrm{mod}\, n)$ for a set of a generating all of $(\mathbb{Z}/n\mathbb{Z})^\times$. If one is happy to assume the Generalised Riemann Hypothesis[1] (GRH), the following result can be used to do the job in polynomial time.

THEOREM 5.2. *Assume GRH. Then $(\mathbb{Z}/n\mathbb{Z})^\times$ is generated by the elements $1, 2, \dots, \lceil 2(\log n)^2 \rceil$.*

We remarked earlier that the computation of $a^{(n-1)/2} (\mathrm{mod}\, n)$ is not especially expensive, and can be done by repeated squaring. Assuming GRH, the whole algorithm works in polynomial time.

5.5. *Fermat numbers

There are many primality tests which work for numbers of a specific type. Perhaps the most famous of these are the Mersenne Primes, primes of the form $M_p = 2^p - 1$ (exercise: if $2^n - 1$ is prime, then n is prime). It is usually the case that the world record largest prime is a Mersenne Prime. The current record is $M_{74207281}$. It is easier to test a number of the form M_p for primality because of the *Lucas-Lehmer test*. You can easily look up the statement of this test, but the analysis (though not terribly difficult) is beyond the scope of this course.

We will illustrate the point that certain specific types of number are easier to test for primality with a different example.

The kth Fermat number, F_k, is defined to be $2^{2^k} + 1$.

PROPOSITION 5.2 (Pepin's test). *Suppose that $n = F_k$, $k \geqslant 1$. Then n is prime if and only if $3^{(n-1)/2} \equiv -1 (\mathrm{mod}\, n)$.*

Proof. Suppose first that the congruence holds. Then certainly $3^{n-1} \equiv 1 (\mathrm{mod}\, n)$. However, as we remarked earlier, conditions like this do not imply that n is prime

[1]The statement that all nontrivial zeros of all Dirichlet L-functions $L(s, \chi)$ lie on the line $\Re s = \frac{1}{2}$. You can find a precise statement online in many places.

(the smallest base 3 pseudoprime is 91: $3^{90} \equiv 1 (\mathrm{mod}\, 91)$). However, it does follow that the order $\mathrm{ord}_n(3)$ divides $n-1$. Moreover, since $3^{(n-1)/2} \equiv -1 (\mathrm{mod}\, n)$, $\mathrm{ord}_n(3)$ does not divide $(n-1)/2$. Since $n-1$ is a power of two, it follows that $\mathrm{ord}_n(3) = n-1$. In particular, the order of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ is (at least) $n-1$, which implies that n is prime.

Conversely, suppose that n is prime. Evidently $n \equiv 1 (\mathrm{mod}\, 4)$. By the reciprocity law we have $\left(\frac{3}{n}\right) = \left(\frac{n}{3}\right)$. Moreover, $n \equiv 2 (\mathrm{mod}\, 3)$; indeed the powers of two alternate between 1 and $2 (\mathrm{mod}\, 3)$, with $2^{2j} \equiv 2 (\mathrm{mod}\, 3)$ and $2^{2j+1} \equiv 1 (\mathrm{mod}\, 3)$. Therefore $\left(\frac{n}{3}\right) = \left(\frac{2}{3}\right) = -1$. The claim now follows from Euler's criterion. □

This test does not provide a useful way of finding large explicit primes, for the simple reason that it is speculated that F_k is composite for $k \geqslant 5$ (and this has been checked for $5 \leqslant k \leqslant 32$).

CHAPTER 6

Public key cryptography

6.1. Introduction

The RSA Public Key Cryptosystem, invented by Rivest, Shamir and Adleman in 1977 allows messages to be sent securely without the need to exchange a "key" secretly. (The algorithm was first discovered in 1974 by the mathematician Clifford Cocks at GCHQ, but this was kept secret until 1997.)

Following tradition, let us suppose that we have two people named Alice and Bob, and that Alice wants to send a message to Bob.

A malicious eavesdropper will appear later by the name of Eve.

6.2. Protocol – Bob

Bob chooses two large primes p and q and an integer e such that $(e, \phi(n)) = 1$. (Note that $\phi(n) = (p-1)(q-1)$, so this is equivalent to $(e, p-1) = (e, q-1) = 1$.) Typically p, q have hundreds of digits each. It is best not to choose them to have any particular structure (for example, choosing Mersenne Primes would be bad). A sensible procedure would be to simply pick numbers at random within a certain range $[M, 2M]$ until one finds two primes, testing each candidate using, say, the Miller–Rabin test. It follows from the prime number theorem (not discussed in this course) that a randomly selected integer from $[M, 2M]$ is prime with probability $\sim 1/\log M$, which is quite large, so this is actually a very sensible way to proceed.

Bob forms the product $n = pq$ and announces the numbers n and e publicly. He *does not* publish the numbers p and q separately.

6.3. Protocol – Alice

Now we describe how Alice sends her message. Suppose the message is written in English. First it must be converted to numerical form. This is done using a suitable numerical substitution scheme such as $A \to 01$, $B \to 02$, etc. This string of numerals is then split into chunks, each of which is a number $< n$. Each of these chunks is then transmitted separately.

If M is one of the chunks, it is transmitted as follows. Alice computes $M^e \pmod n$ (by which we mean M^e, reduced modulo n to lie in $\{0, \ldots, n-1\}$) and sends this to Bob.

6.4. Decryption

Now Bob has the encrypted message $M^e (\mathrm{mod}\, n)$. How does he decrypt it? Since Bob knows p and q, he can compute $\phi(n) = (p-1)(q-1)$. Since, by assumption, e is coprime to $\phi(n)$, he can find d such that

$$de \equiv 1 (\mathrm{mod}\, \phi(n))$$

(by Euclid's algorithm), say $de = k\phi(n) + 1$. But then

$$(M^e)^d = (M^{\phi(n)})^k M.$$

By the Fermat–Euler theorem, this is $\equiv M (\mathrm{mod}\, n)$.

However, the unencrypted message M is known to be a natural number $< n$, and so this allows it to be recovered uniquely.

There is an issue here if it happens that M is not coprime to n. However, since $n = pq$ with p and q large primes, this is exceptionally unlikely to happen.

6.5. Security

The decryption method we presented above depends on having the number d to hand. To calculate this, we needed $\phi(n)$. Eve, the eavesdropper, could read the message if she had $\phi(n)$.

However, knowledge of $\phi(n)$ is equivalent to knowledge of the factorisation $n = pq$, which is widely believed to be hard. Indeed, since

$$p + q = pq - (p-1)(q-1) + 1 = n - \phi(n) + 1,$$

the factors p and q may be recovered as the roots of the quadratic equation

$$x^2 - x(n - \phi(n) + 1) + n = 0.$$